The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
02/04/2013

SUBJECT:
Oracle Java Runtime Environment (JRE) is prone to multiple security vulnerabilities.

OVERVIEW:
Multiple vulnerabilities have been discovered in Oracle Java Runtime Environment (JRE) that can lead to remote code execution. The Java Runtime Environment is used to enhance the user experience when visiting websites and is installed on most desktops and servers. This vulnerability may be exploited if a user visits or is redirected to a specifically crafted web page. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the JRE application. Depending on the privileges associated with the application, an attacker could execute arbitrary code in the context of the application, bypass security restrictions, or cause denial-of-service conditions; other attacks may also be possible.

SYSTEM AFFECTED:
- Oracle Java SE JDK and JRE 7 Update 11 and earlier
- Oracle Java SE JDK and JRE 6 Update 38 and earlier
- Oracle Java SE and JRE 5.0 Update 38 and earlier
- Oracle Java SE SDK and JRE 1.4.2_40 and earlier
- Oracle Java SE JavaFX 2.2.4 and earlier

RISK:

Government:
- Large and medium government entities: High
- Small government entities: High

Businesses:
- Large and medium business entities: High
- Small business entities: High

Home users: High

DESCRIPTION:

Multiple vulnerabilities have been discovered in Oracle Java Runtime Environment that can lead to remote code execution. In order to exploit these vulnerabilities, an attacker must first create a web page with a specially crafted applet designed to leverage this issue. When the web page is visited, the attacker supplied code is run in the context of the affected application.

Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the JRE application. Depending on the privileges associated with the application, an attacker could execute arbitrary code in the context of the application, bypass security restrictions, or cause denial-of-service conditions; other attacks may also be possible.

RECOMMENDATIONS:

The following actions should be taken:

- Apply the patch from Oracle, after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.

REFERENCES:

Security Focus:

http://www.securityfocus.com/bid/57670

Oracle:

http://www.oracle.com/technetwork/topics/security/javacpufeb2013-1841061.html